

Niko Luoto

Bluetooth Low Energy- ja ZigBee- verkkotekniikoiden hyödyntäminen kotiauto- maatiassa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinööriytyö

15.4.2016

Tekijä Otsikko	Niko Luoto Bluetooth Low Energy- ja ZigBee- verkkotekniikoiden hyödyntäminen kotiautomaatiossa
Sivumäärä Aika	32 sivua 15.4.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Sulautettu tietotekniikka
Ohjaaja	Lehtori Anssi Ikonen
<p>Insinööriyön tarkoituksena oli vertailla kahta kotiautomaatiossa käytettävää verkkotekniikkaa, Bluetooth Low Energyä (BLE) ja ZigBeetä keskenään, koska kotiautomaatiomarkkinat ovat kasvussa ja näitä järjestelmiä tulee yhä enemmän yksityishenkilöiden käyttöön. Insinööriyöraportti on tarkoitettu henkilöille, jotka ovat kiinnostuneita näistä tekniikoista ja mahdollisesti suunnittelemassa kotiautomaatioverkkoa tai sellaisen ostamista.</p> <p>Työ alkoi tutkimalla BLE:n tietoturvaa ja siihen liittyviä mekanismeja sekä BLE:n verkkotopologioita ja protokollapinoa. Selvisi, että BLE on suljettu ja melko yksinkertainen järjestelmä. Se on myös jo laajalti käytössä muualla kuin kotiautomaatiossa, muun muassa matkapuhelimissa. Tämän jälkeen tutkin ZigBeetä samoin kuin BLE:tä, käyttäen samoja aihealueita kuin edellä eli tietoturvaa, verkkotopologioita ja toimintaa. Selvisi, että ZigBee on avoin järjestelmä, joka on pääosin teollisuudessa käytössä.</p> <p>ZigBeellä tehtiin esimerkkitoteutus käyttäen kahta XBee-nodea, LabVIEW-ohjelmaa käyttöliittymänä ja LM35-lämpötilasensoria. Siinä selvitettiin järjestelmien yhteensopivuus ja mahdollisesti ilmeneviä ongelmia. Lopputuloksena valmistui verkko kahdella nodella, joista toinen vastaanotti datan LM35-sensorilta ja lähetti sen vastaanottavalle nodelle, mistä tieto siirtyi LabVIEW-ohjelmalle. Näin saatiin käytännössä yksi mahdollinen kotiautomaatioverkon toteutustapa ja sitä pystyisi jatkossa laajentamaan.</p> <p>Lopputuloksena selvisi, että molemmat järjestelmät sopisivat kotiautomaatioon. Ne pystyvät tekemään samaa asiaa, mutta ovat sen verran erilaiset, että käytännössä niille sopii eri käyttökohteet.</p>	
Avainsanat	BLE, ZigBee, kotiautomaatio, LabVIEW

Author Title Number of Pages Date	Niko Luoto Making use of Bluetooth Low Energy and ZigBee in home automation 32 pages 15 April 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Embedded Systems
Instructor	Anssi Ikonen, Senior Lecturer
<p>The purpose of this thesis was to compare two home automation network technologies. They are Bluetooth Low Energy (BLE) and ZigBee. This is because the home automations market is growing and it is becoming more and more available to everyone. This thesis is meant for everyone who is interested in home automation or who designs these systems.</p> <p>The study began by research on Bluetooth Low Energy. First, security, network topologies and protocol stacks were researched. It was found out that BLE is a closed and rather simple system. It is widely used in other systems, for example on mobile phones. After BLE was studied, ZigBee was investigated in the same way. The same issues were covered than previously. They were security, network topologies and protocols. It was found out that ZigBee is open source and that it is mainly used in industry.</p> <p>An example network was made by using two XBee nodes, the LabVIEW program as an interface and a LM35 temperature sensor. The purpose of this example was to find any compatibility problems. The end result of this was a network with two nodes where one node received data from the LM35 sensor and sent the information to another node which transferred the data to the LabVIEW program. This way one can create a working, small home automation network that can be expanded afterwards.</p> <p>As a result, it became clear that both systems would be suitable for home automation. Both systems can be used basically in the same tasks but in reality they are best suited for different usage.</p>	
Keywords	BLE, ZigBee, home automation, LabVIEW

Sisällys

Lyhenteet

1	Johdanto	1
2	Bluetooth Low Energy -langaton lähiverkkotekniikka	1
2.1	Bluetooth smart (BLE)	2
2.2	Bluetooth smart ready (BR/EDR/LE)	2
2.3	Classic Bluetooth (BR/EDR)	3
3	Bluetoothin toiminta	4
3.1	Tiedonsiirto	5
3.2	Anturiverkon topologiat	6
3.3	Tietoturva	7
3.4	BLE-kytkeytyminen	8
3.5	BLE-protokollapino	9
4	ZigBee-langaton lähiverkkotekniikka	12
4.1	ZigBeen ominaisuudet	13
4.2	Toimintamuodot	15
4.3	Verkkotopologiat	16
4.4	Tietoturva	18
4.5	XBee-lähetin-vastaanotinmoduuli	19
4.6	XBee-moduulin käyttö ja komennot	20
5	ZigBee ja LabVIEW -kotiautomaatiototeutus	22
5.1	ZigBee-verkon koordinaattorin ja päätelaitteen asetukset	22
5.2	LabVIEW-ohjelma	23
6	BLE:n ja ZigBeen vertailu	24
7	Yhteenveto	28
	Lähteet	29

Lyhenteet

BLE Bluetooth Low Energy, Bluetooth LE tai Bluetooth Smart.

BR/EDR/LE Bluetoothin eri datan lähetys tekniikoita.

SIG Special interest group. Bluetooth-standardia hallinnoiva järjestö.

WPAN/PAN Wireless personal area network/personal area network. Henkilökohtaisen alueen langaton tai langallinen verkko.

ISM Industrial, science and medical. Maailmanlaajuisesti määritetyt vapaat taajuusalueet.

WIFI WLAN - wireless local area network. Langaton lähiverkko.

STK Short term key. Väliaikainen salausavain tiedonsiirtoon.

NFC Near field communication. Kahden laitteen väliseen tiedonsiirtoon tarkoitettu tekniikka lyhyellä matkalla.

DSSS Direct Sequence Spread Spectrum. Datan lähetystekniikka, jossa lähetettävä data jaetaan pieniin osiin ja lähetetään koko taajuusalueella kerralla.

QPSK Quadrature Phase Shift Keying. Neljän kantaallon modulaatiotekniikka.

BPSK Binary Phase Shift Keying. Kahden kantaallon modulaatiotekniikka.

CSMA/CA Carrier Sense Multiple Access With Collision Avoidance. Siirtotien varausmenetelmä, jossa on törmäyksen esto.

DIFS Distributed interframe space. ZigBee-laitteelle määriteltävä viive, jonka se odottaa tarvittaessa.

AES Advanced Encryption Standard. Salausmenetelmä, jota ZigBee ja BLE käyttävät.

1 Johdanto

Opinnäytetyön tarkoituksena on vertailla kahta kotiautomaatiossa käytettävää lyhyen kantaman anturiverkon toteutustapaa. Työssä toteutetaan ZigBeetä ja LabVIEW'tä käyttämällä konkreettinen esimerkki, jonka avulla tutkitaan verkon toteutusta ja toimintaa. Työn aiheen valitsin sen kiehtovuuden ja tulevaisuuden potentiaalin takia, koska kotiautomaatiossa otetaan isoja askelia eteenpäin. Vuosien päästä varmasti ollaan pisteessä, että kaikkea kotona sähköllä toimivaa voi hallita verkon kautta.

Teen työn oppilaitoksen kanssa yhteistyössä ja pääosin työskentelen kotoa käsin. Työssäni yritän avata kahden yleisen teknologian, ZigBeen ja Bluetooth Low Energyn toimintaa ja mahdollisia käyttökohteita. Lopussa vertailen näitä kahta järjestelmää ja työn perusteella tutkin niille sopivia eri käyttökohteita.

2 Bluetooth Low Energy -langaton lähiverkkotekniikka

Bluetooth Low Energy, joka tunnetaan myös nimillä BLE, Bluetooth LE ja Bluetooth Smart, on osa Bluetooth 4.0 -standardia. Siihen kuuluvat myös Classic Bluetooth- ja Bluetooth high speed -protokollat, joita ei käsitellä tässä raportissa. Bluetooth LE on saanut alkunsa Nokian kehittämästä langattomasta tiedonsiirtotekniikasta nimeltään Wibree. Nokia aloitti sen kehittämisen vuonna 2001, ja vuonna 2006 SIG ilmoitti ottavansa Wibreen osaksi Bluetooth low energy -standardia. [1; 2; 3.]

BLE on langaton tiedonsiirtotekniikan protokolla, joka on tarkoitettu pienitehoisten ja lyhyen viiveen omaavien laitteiden väliseen kommunikointiin. Se kehitettiin erityisesti, jotta voitaisiin lähettää dataa pienemmällä virrankulutuksella perinteiseen Bluetoothiin verrattuna. Tämä on saavutettu pienentämällä kantamaa ja lähetettävän datan määrää. [4.]

BLE:n kantama riippuu paljon monesta eri tekijästä, muun muassa ympäristöstä, antennista ja kotelosta. Sillä on kuitenkin mahdollista saavuttaa yli 300 metrin kantama akun keston kustannuksella. Tavallisesti BLE:n kantama on muutamia metrejä, jolloin säilytetään sen tärkein ominaisuus eli vähäinen virrankulutus. [4.]

Lähetettävän datan määrää saatiin pienennettyä huomattavasti yksinkertaistamalla protokollaa. Normaalioloissa BLE lähettää dataa 5–10 kbps ja Classic Bluetooth 3–25 Mbps.

Vuonna 2011 käyttöön otettiin uudet logot, joista tunnistaa Bluetooth LE -yhteensopivat laitteet: Classic Bluetooth, Bluetooth smart ja Bluetooth smart ready.

2.1 Bluetooth smart (BLE)

BLE-logon (kuva 1) omaava laite on niin sanottu single mode-laite. Fyysisesti tämä laite on yleensä pieni ja paristolla toimiva. Single-mode tarkoittaa sitä, että se pystyy kommunikoimaan ainoastaan toisen single-mode-laitteen kanssa (kuva 4). Se siis tukee vain BLE-protokollaa. Tästä on hyötynä se, että laite kuluttaa vähän virtaa ja on kooltaan pieni. [6.]



Kuva 1. Bluetooth Smartin logo [5].

Bluetooth LE -laite pystyy olemaan päällä teoriassa jopa 7 vuotta, mutta käytännössä se riippuu monesta eri tekijästä, kuten akusta, datan lähetyksen aikavälistä ja laitteiden etäisyydestä [7]. Tällä hetkellä markkinoilla olevia BLE -tekniikkaa käyttäviä tai BLE -tekniikkaan perustuvia laitteita ovat muun muassa erilaiset älyvaatteet, sykemittarit ja tietokoneen hiiret. [8.]

2.2 Bluetooth smart ready (BR/EDR/LE)

Bluetooth smart ready -laite (kuva 2) on niin sanottu dual mode -laite, eli siinä on niin classic bluetoothin kuten BLE:n protokollat. Tällainen laite pystyy kommunikoimaan sekä classic Bluetooth -protokollaa käyttävän laitteen kanssa että Bluetooth smart- ja

smart ready protokollaa -käyttävän laitteen kanssa (kuva 4). Ominaisuuksien lisääntyessä laitteen koko ja virrankulutus kasvavat, joten näin ei päästä BLE:n tyypilliseen pieneen virrankulutukseen. Dual mode -laitteilla pitää olla myös huomattavasti isompi akku kuin BLE:n tekniikan omaavilla laitteilla, tai laite pitää olla kytkettynä verkkovirtaan. Tämän tekniikan sisältäviä laitteita ovat muun muassa puhelimet, tabletit ja tietokoneet. [8; 6.]



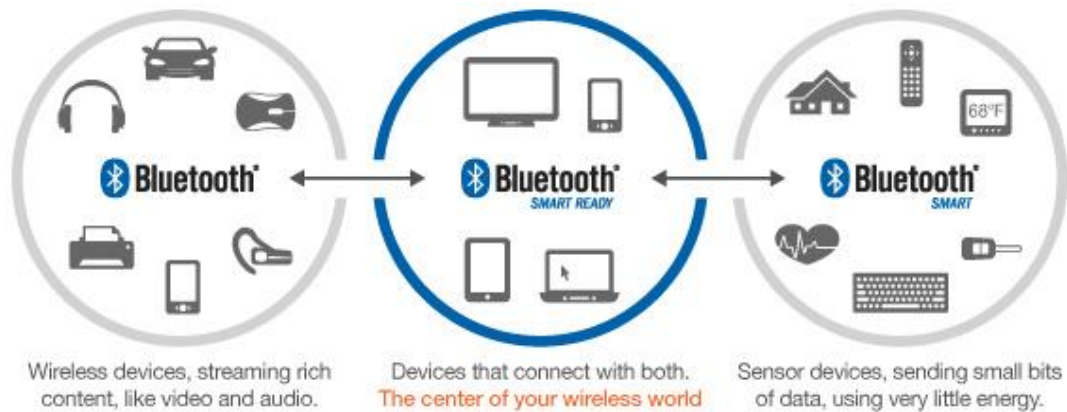
Kuva 2. Bluetooth Smart Readyn logo [5].

2.3 Classic Bluetooth (BR/EDR)

Classic Bluetooth -laite (kuva 3), tai yleisemmin tunnettuna vain Bluetooth, pystyy kommunikoimaan smart ready- tai toisen classic bluetooth -protokollan omaavan laitteen kanssa (kuva 4). Classic Bluetooth -laitteita ovat muun muassa handsfreet, kuulokkeet ja tulostimet. [8; 9.]



Kuva 3. Classic Bluetooth logo [5].



Kuva 4. Bluetooth-järjestelmän ekosysteemi [10].

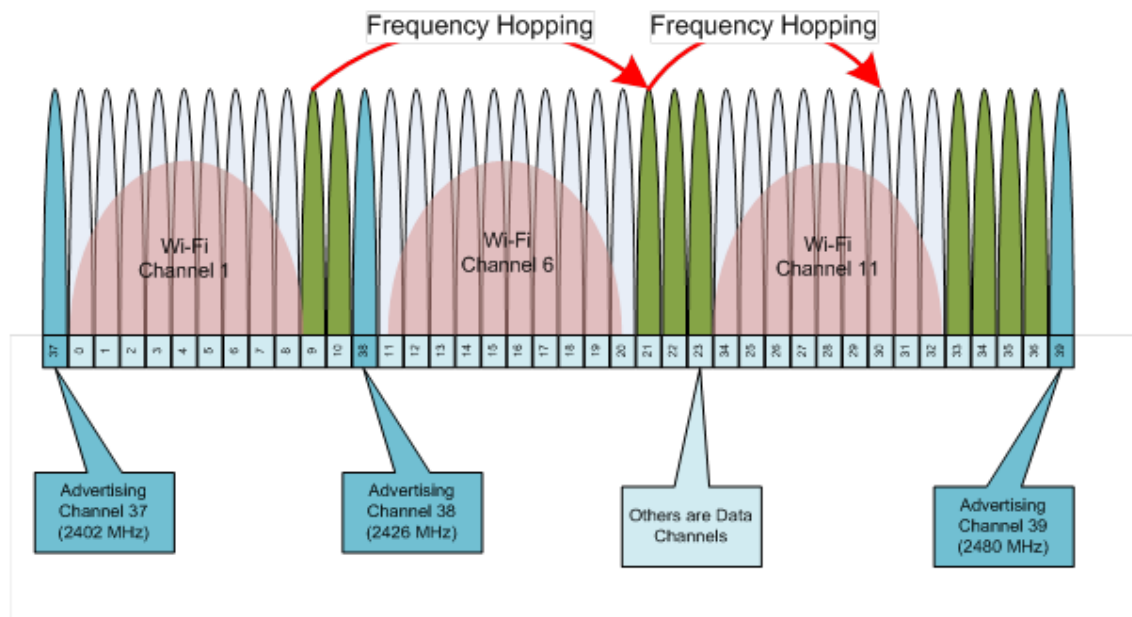
3 Bluetoothin toiminta

Bluetooth-standardin kehitti Ericsson (nykyinen Sony Mobile Communications) vuonna 1994. Se kehitettiin alun perin langattomaksi vaihtoehdoksi tietokoneiden, puhelinten ja tulostinten välille. Vuonna 1998 Ericssonin aloitteesta Ericsson, Intel, Nokia, Toshiba ja IBM perustivat yhdessä Bluetooth Special Interest Group -nimisen järjestön, jonka hallittiin hallitsevan Bluetooth-standardia. Järjestön tarkoituksena on valvoa ja lisensoida Bluetooth-tekniikkaa ja -tavaramerkkiä valmistajille. Bluetooth 4.0 on vuonna 2010 Bluetooth SIG:n esittelemä uusien Bluetooth-teknologiastandardi, ja siihen kuuluu BLE. Ensimmäiset tätä teknologiaa hyödyntävistä tuotteista saapuivat markkinoille vuoden 2011 aikana [11].

Bluetoothin toimintaperiaate on yksinkertainen. Sen tarkoituksena on siirtää pieniä määriä dataa kerralla lyhyellä matkalla käyttäen radioaaltoja ja samalla kuluttaa mahdollisimman vähän virtaa. BLE:n toiminta-alueena katsotaan yleensä olevan niin sanottu langaton henkilökohtainen verkko eli WPAN (wireless personal area network).

Bluetooth LE, kuten Classic Bluetooth, käyttää 2.400–2.4835 GHz ISM -taajuutta, pois lukien Ranska, Espanja ja Japani. BLE:ssä on 40 kahden megahertsin kanavia toisin kuin classic Bluetoothissa, joka käyttää 79:ää yhden megahertsin kanavia. Näistä 40:stä 37 kanavaa on datan lähetystä varten ja kolme on yhteyden muodostamista varten. Näitä kolmea yhteydenmuodostamiskanavaa, joita kutsutaan mainostuskanaviksi (2402, 2426, 2480 MHz), käytetään toisten BLE-laitteiden etsimiseen, yhteydenmuodostusparametrien vaihtamiseen ja broadcast-tyyppisen datan lähetykseen. Ne

on sijoitettu niin, ettei samalla taajuusalueella oleva WIFI-verkko häiritsisi niitä [12] (kuva 5).



Kuva 5. BLE:n taajuuskanavat ja mainostuskanavat wifi-kanavien rinnalla [12].

BLE-laite kuluttaa käytössä erittäin vähän virtaa. Sen vähäinen virrankulutus perustuu pääasiassa siihen, että se lähettää pieniä paketteja lähelle nopeassa rytmissä. Esimerkiksi classic Bluetooth lähettää datan 100 ms:ssa, kun taas BLE lähettää sen alle 6 ms:ssa.

3.1 Tiedonsiirto

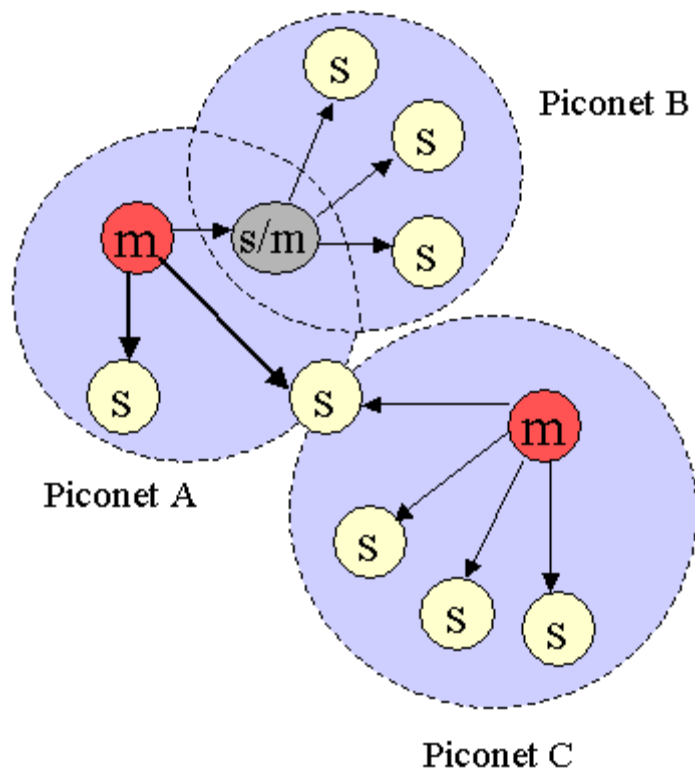
Bluetoothissa datansiirto tapahtuu taajuushyppelyyn perustuvalla hajaspektritekniikalla, joka tunnetaan nimellä Frequency Hopping Spread Spectrum eli FHSS (kuva 5). Siinä nimen mukaisesti hypitään kanavalta toiselle ennalta sovitun algoritmin mukaisesti ja samalla lähetetään dataa. Tämä tekniikka vähentää taajuuksilla ilmenevien häiriöiden vaikutusta yhteyden ylläpitämiseen. Taajuushyppelyalgoritmi sovitetaan mainostuspaketien vaihdon yhteydessä.

Hajaspektri kehitettiin alkuun ainoastaan sotilas- ja tiedustelukäyttöön. Vuonna 1985 ratifioitiin kuitenkin kansainvälinen sopimus, jossa vapautettiin kolmen ISM-

taajuusalueen (Industrial, Scientific and Medicine), 902–928 MHz, 2,4000–2,4835 GHz ja 5,725 - 5,850 GHz, hajaspektritekniikkaan perustuvan lisenssivapaa käyttö.

3.2 Anturiverkon topologiat

BLE-protokolla perustuu point-to-point-yhteyteen. Tätä voidaan laajentaa määrittämällä yksi node master-nodeksi ja muodostamalla star-bus-verkkotopologia. Bluetooth-verkkotopologiasta puhuttaessa käytetään yleisemmin nimityksiä piconet ja scatternet. Piconet koostuu vähintään kahdesta BLE-laitteesta ja scatternet koostuu kahdesta tai useammasta piconetistä (kuva 6).



Kuva 6. Kolme piconetiä (A, B, C) ja yhdessä kaikki muodostavat scatternetin (m = master, s = slave ja s/m = master ja slave) [15].

Piconet

Piconet on kahden tai useamman BLE-laitteen välinen yhteystapa. Se tunnetaan tavallisemmin star-bus-verkkotopologiana. Piconetissä skannaava laitetta kutsutaan masteriksi ja muita slaveksi (kuva 6). Master-laitteen vastuulla on antaa jokaiselle slave-laitteelle oma taajuushyppelyalgoritmi (FHSS), jolloin vältetään keskinäisiä törmäyksiä.

Master-laite välittää vielä loput tarvittavat tiedot yhteyden muodostamista varten. Piconetissä on 3 bitin kokoinen osoiteavaruus, joka rajoittaa aktiivisten laitteiden kokonaisuuden yhdessä piconetissä kahdeksaan kappaleeseen ($2^3 = 8$). Master-laitteen lisäksi voi olla enintään seitsemän slave-laitetta. Master-laite voi kuitenkin määrätä slave-laitteita lepotilaan, ja silloin niitä voi olla enimmillään 248 edellä mainitun seitsemän slave-laitteen lisäksi. Nämä nukkuvat laitteet herätetään master-laitteen käskystä, mutta sitä ennen yhden aktiivisen slave-laitteen on mentävä lepotilaan, jotta uudelle laitteelle tulee tilaa. [3; 13.]

Scatternet

BLE:n versioon 4.1 on otettu mukaan dual mode -ominaisuus, eli laitteella voi olla kaksi roolia. Roolit ovat aina eri verkoissa, eli laite voi olla master-laite yhdessä piconetissä ja slave-laite toisessa tai kahdessa eri piconetissä. Laite voi kuitenkin olla ainoastaan master-laitteena yhdessä piconetissä. Näin BLE kykenee muodostamaan scatternet-verkkotopologian. Se syntyy, kun kaksi tai useampia piconet-verkkoja yhdistyy toisiinsa. Bluetooth Smart Mesh Working Group on parhaillaan kehittämässä tukea mesh-verkkotopologialle. [3; 13; 14.]

3.3 Tietoturva

Bluetoothin tietoturvasta vastaa security manager. Se on protokolla, joka on luotu mahdollistamaan Bluetooth-protokollapinin luovan ja vaihtavan suojausavaimet. Se huolehtii myös toisen laitteen luotettavuudesta ja tarpeen vaatiessa piilottaa Bluetooth-osoitteen. Security manager mahdollistaa kolme menettelytapaa. Kaikki edellä mainittu salaus tapahtuu 128 bittistä AES-standardia käyttäen. [3.]

Aina ensimmäiseksi tehdään kahden laitteen paritus (pairing). Tällä menettelytavalla saadaan luotua väliaikaiset salausavaimet ja pystytään luomaan salattu yhteys. Tämän jälkeen laitteet liitetään yhteen (bonding). Siinä luodaan ja vaihdetaan lopulliset salausavaimet ja luodaan lopullinen yhteys. Lopuksi vielä vahvistetaan salaus uudelleen (Encryption Re-establishment), jolla määritetään, miten juuri luotuja avaimia käytetään tulevien yhteyden luomisten aikana. Tämän jälkeen paritusta ja yhteen liittämistä ei tarvitse enää jatkossa tehdä ja saadaan luotua turvallinen ja salattu yhteys nopeammin seuraavilla kerroilla. [3; 16.]

Tietoturvan ensimmäinen vaihe eli paritus loppuu aina juuri luotujen salausavainten luomaan salattuun yhteyteen. Tähän päästäkseen osapuolet sopivat kolmesta vaihtoehdosta, miten väliaikainen salausavain (short term key eli STK) luodaan:

”Just Works” -menettely on turvattomin. Siinä molemmat osapuolet luovat salausavaimen aikaisemmin vaihdetusta plain text -datasta. Tässä tapauksessa man-in-the-middle hyökkäystä ei pystytä torjumaan, kuten kahdessa seuraavassa vaihtoehdossa.

”Passkey Display” -menettelyssä toinen osapuoli luo sattumanvaraisen 6 numeron sarjan, joka käyttäjää pyydetään sitten syöttämään yhdistettävään laitteeseen.

”Out Of Band” -menettelyvaihtoehdossa lisätiedot lähetetään jokin muuta kuin BLE:n radiotien kautta, esimerkiksi NFC:tä hyväksi käyttäen. [3.]

3.4 BLE-kytkytyminen

BLE:llä on vain kaksi erityyppistä pakettia, mainos- ja datapaketti. Tämä yksinkertaistaa protokollapinon muotoa huomattavasti ja näin ollen vähentää laitteen tarvitsemia yhteystiloja ja virran kulutusta. [3.]

Mainospaketilla on kaksi tarkoitusta. Ensimmäinen tarkoitus on löytää slave-laite ja luoda yhteys siihen. Toinen tarkoitus on datan lähettäminen broadcast-tilassa kaikille niille, jotka eivät tarvitse täyden yhteyden muodostamisen hyötyjä. [3.]

Mainospaketit ovat kooltaan 6–37 tavua. Ne lähetetään ennalta määrätyn ajan välein (20 ms–10,24 s), jotta skannaavan laitteen olisi mahdollista löytää mainostaja. Mainostamiseen käytetään kolmea kanavaa, jotka on aseteltu taajuusalueelle siten, että WiFi:n kanavat häiritsisivät niitä mahdollisimman vähän, mikä vähentää häiriön mahdollisuutta näiden kanavien taajuudella. Mainostajaa ja skannaajaa ei ole millään lailla synkronoitu toistensa kanssa, joten ne löytävät toisensa vain sattumalta kohdatessaan samalla taajuudella. [3.]

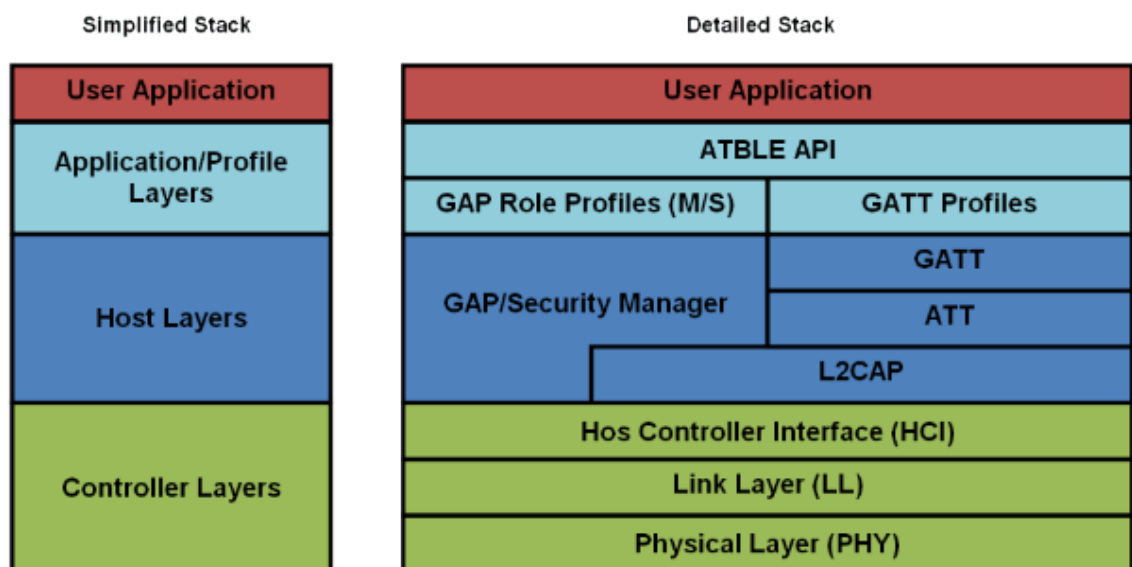
Yhteyden luominen lähtee siitä, että master-laite alkaa skannata taajuusaluetta löytääkseen slave-laitteita, jotka mainostavat itseään ja hyväksyvät yhteyden muodostamisen. Kun sopiva laite löytyy, master-laite lähettää yhteydenmuodostamispaketin. Kun

slave-laite vastaa, yhteys on muodostettu. Paketti, jonka master-laite lähettää, sisältää tiedon taajuushyppelyn sekvenssistä, jota molemmat laitteet seuraavat koko yhteydessäoloajan. Yhteyden muodostamisessa master-laite lähettää vielä kolme yhteysparametriä, jotka ovat seuraavat:

- ”Connection interval” on aika kahden peräkkäisen yhteystapahtuman välillä (7,5 ms–4 s).
- ”Slave latency” -numero määrittää sen, montako yhteystapahtumaa päälaitte voi jättää väliin ilman, että yhteys katkeaa.
- ”Connection supervision timeout” on numero, joka määrittää pisimmän ajan, jonka jälkeen laitteet katkaisevat yhteyden, jos eivät saa voimassa olevaa pakettia toiselta. [3; 16.]

3.5 BLE-protokollapino

Bluetooth low energy -protokollapino (kuva 7) toimitetaan ohjelmiston mukana suljettuna lähdekoodina, ja silloin siihen ei pääse käsiksi. Protokollapinon käyttämistä varten omassa ohjelmassa käyttäjän täytyy ymmärtää GAP- ja GATT-profiilien toiminta. Kommunikointi protokollapinon kanssa tapahtuu niiden avulla. [3.]



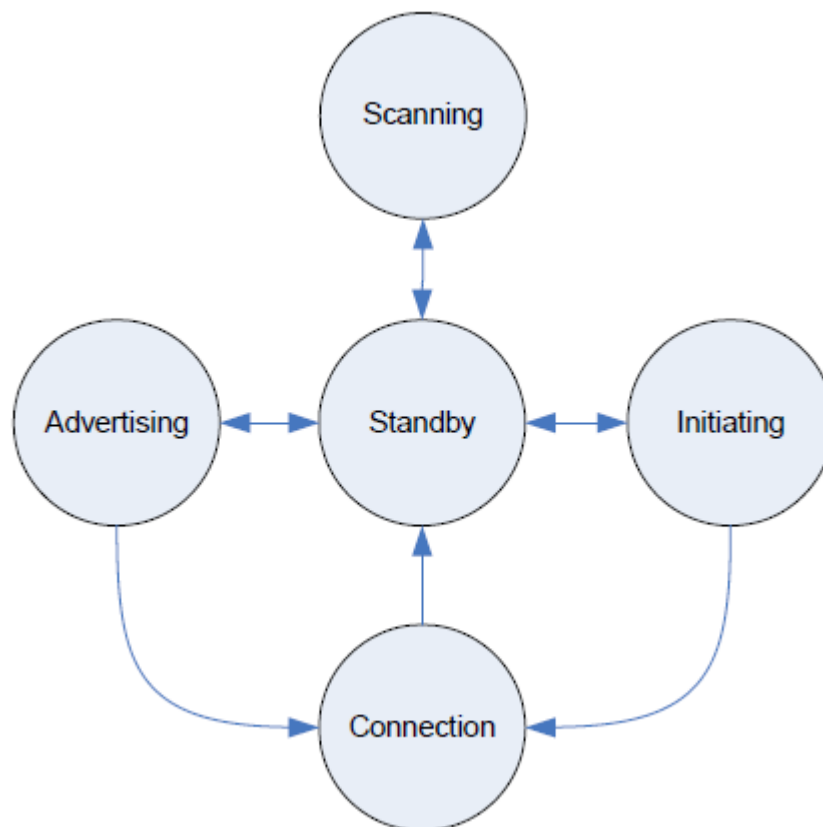
Kuva 7. Bluetoothin protokollapino yksinkertaistettuna vasemmalla ja avattuna oikealla [17].

Physical Layer (PHY)

Physical Layer on nimensä mukaan fyysinen kerros, jossa vastaanotetaan ja lähetetään analoginen signaali. Kerroksessa myös muunnetaan vastaanotettava signaali analogisesta muodosta digitaaliseen tai lähetettävä signaali päinvastoin. [3.]

Link Layer (LL)

Link layer on käytännössä tilakone (kuva 8), mutta se myös vastaa pakettien ja radion ohjauksesta. Sillä on käytössä viisi eri tilaa, joissa se voi olla. Nämä tilat ovat standby, advertising, scanning, initiating tai connected. Tiloja voi olla aktiivisena vain yksi kullakin hetkellä.



Kuva 8. Bluetooth low energyn kaikki käytössä olevat tilat [18].

Standby-tilasta laite aloittaa, kun se käynnistetään, ja se pysyy siinä niin kauan, kunnes se saa käskyn host-rajapinnasta siirtyä toiseen tilaan. Standby-tilassa laite ei voi lähettää eikä vastaanottaa dataa. Tässä tilassa BLE-laitteen virrankulutus saadaan todella alhaiseksi.

Advertising-tilassa laite lähettää mainospaketteja kertoakseen, että on valmis luomaan yhteyden. Se voi myös tässä tilassa vastata saapuneisiin yhteydenmuodostuspyyntöihin.

Scanning-tilassa laite aktiivisesti skannaa mainostuspaketteja lähettäviä laitteita. Pelkästään mainostuspaketteja vastaanottava laite on passiivisessa skannaustilassa. Olllessaan aktiivisessa skannaustilassa laite aloittaa yhteydenmuodostamisen, kun se saa mainostuspaketin.

Initiating-tilassa on ensimmäiset mainostuspaketit lähetetty ja vastaanotettu, ja tässä tilassa odotetaan lisätietoja yhteyden muodostamista varten samaiselta mainostuskanavalta.

Connected-tilaan päästään, kun kaksi laitetta on luonut yhteyden toisiinsa. Yhteyden luoneesta laitteesta tulee master-laite ja yhteyden hyväksyneestä laitteesta slave-laite. [3.]

Host-Controller Interface (HCI)

HCI on rajapinta esimerkiksi PC:n tai puhelimen käyttöjärjestelmän ja BLE:n mikropiirin väliseen kommunikointiin. Esimerkiksi tietokoneessa ohjelma on päällä ja bluetooth-moduuli kiinnitetään tietokoneeseen käyttämällä USB-porttia, jolloin USB on rajapintana. [3.]

Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP:lla on kaksi eri toimintoa. Se toimii rajapintana ylemmille protokollille, ja se pilkkoo datan pienempiin paketteihin lähetystä varten ja kokoaa taas vastaavasti vastaanotetun datan luettavaan muotoon ylemmille kerroksille. [3.]

Security Manager

Security Manager huolehtii BLE-laitteiden salauksesta. Se salaa laitteiden välisen liikenteen ja hallitsee salausavaimia tarvittaessa sekä todentaa laitteita. [3.]

Generic Acces Profile (GAP)

GAP määrittää, miten laitteet kommunikoivat alemmilla kerroksilla toistensa kanssa ilman määrättyä protokollaa muun muassa tilanteessa, joissa on kaksi eri valmistajan laitetta. Sitä voidaan pitää tärkeimpänä BLE-protokollan hallinnointikerroksena. GAP kontrolloi menettelyjä, joilla hallitaan laitteiden löytymistä, yhdistämistä, salauksen perustamisesta sekä muita menettelyjä, joilla luodaan puitteet datan liikkumiselle. [3]

Attribute Protocol (ATT)

ATT-protokolla luotiin BLE-laitteita varten. Se on yksi osa-alue, joka mahdollistaa pienen virrankulutuksen. ATT-protokolla tuo mahdollisuuden datan paljastamiseen toiselle laitteelle. Paljastettua dataa kutsutaan attributes-nimellä. Näitä paljastava laite on server ja vastaanottava on client. Master- ja slave-rooleilla ei ole mitään merkitystä tämän kanssa. Tämä järjestely mahdollistaa nopean ja alhaisen virrankulutuksen tiedonsiirrossa. Esimerkiksi lämpötilaa seurattaessa lähetetään tieto vain silloin, kun lämpötila-arvo muuttuu, ja näin ollen ei tarvitse lähettää arvoja tasaisin väliajoin, vaikka lämpötila ei olisi muuttunut. [3.]

Generic Attribute Profile (GATT)

GATT huolehtii ja hallinnoi yhteyden muodostamiseen kuuluvat käskyt ja toimenpiteet. Se myös määrittää, miten dataa järjestetään ja liikutellaan ohjelmien välillä. [3.]

4 ZigBee-langaton lähiverkkotekniikka

ZigBee Alliance on vuonna 2004 kehittänyt ZigBee-standardin (kuva 9) ensimmäisen version. Se on lyhyen kantaman langaton tiedonsiirtotekniikka ja kuuluu WPAN (wireless personal area network) -standardiperheeseen (IEEE 802.15). ZigBeen perustajajäsenet ovat Honeywell, Invensys, Motorola, Mitsubishi, Philips ja Samsung. [19.]



Kuva 9. ZigBeen logo [21].

ZigBee kuuluu tämän standardiperheen kymmenestä eri työryhmästä ryhmään numero 4, jonka standardi on IEEE 802.15.4. Se julkaistiin toukokuussa 2003. Tämä standardi määrittelee OSI-mallista fyysisen ja siirtoyhteyskerroksen. Tähän ryhmään kuuluu pienitehoisia ja suuren akkukeston (kuukaudesta jopa vuosiin) omaavia laitteita. ZigBeen lisäksi ryhmään kuuluvat WirelessHART, 6LoWPAN ja ISA100.11a. [19; 20.]

4.1 ZigBeen ominaisuudet

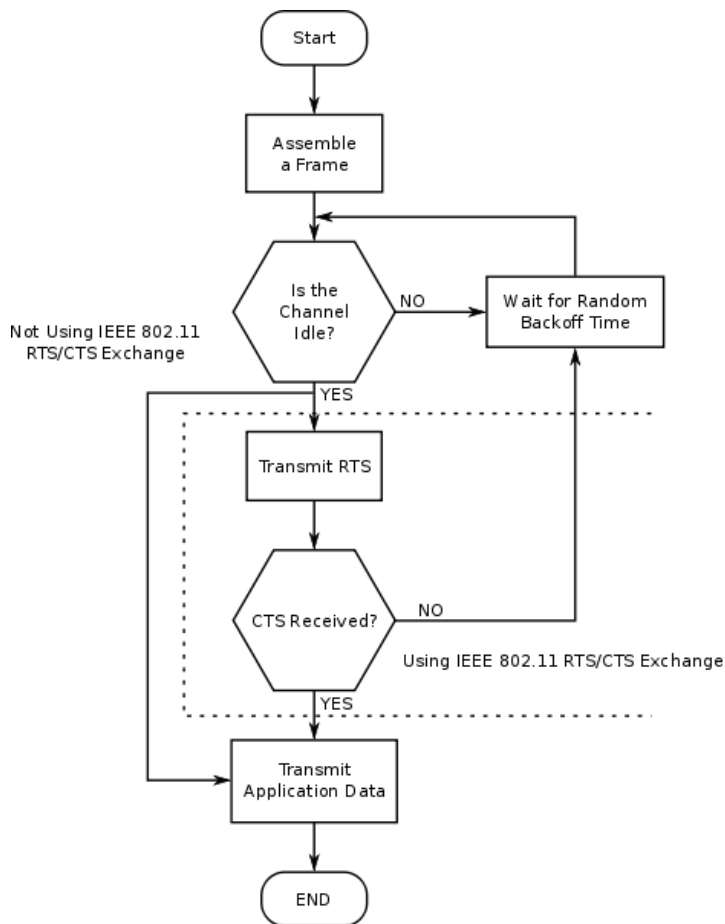
ZigBee on rekisteröity tavaramerkki, jonka omistaja on ZigBee Alliance. Siihen kuuluu joukko yrityksiä, jotka hallinnoivat ja julkaisevat ZigBee-standardeja. ZigBee käyttää Euroopassa ja Japanissa 868 MHz:n taajuutta ja toimii nopeudella 20 kb/s, Yhdysvalloissa ZigBee käyttää taajuutta 915 MHz ja toimii nopeudella 40 kb/s. Maailmanlaajuisista taajuuksista 2,4 GHz voi käyttää missä vain, ja se toimii nopeudella 250 kb/s. Euroopassa taajuudesta on varattu vain yksi kanava. Yhdysvalloissa kanavia on kymmenen 2 MHz:n välein ja maailmanlaajuisesti kuusitoista 5 MHz:n välein. [22; 23.]

ZigBee-laitteiden kantama on kymmenen metrin ja muutaman sadan metrin välillä, riippuen olosuhteista. Sisällä kantama on lyhyempi seinien ja muiden esteiden vuoksi. Pienempien taajuuksien kantama on pitempi, mutta samalla nopeus on alhaisempi. [22.]

ZigBee-verkko voi teoreettisesti koostua jopa yli 15 miljoonasta laitteesta, mutta käytännöllisessä verkossa laitteita voi olla enintään muutamia satoja. Yli tuhannen laitteen verkossa alkaa ilmetä teknisiä ongelmia, esimerkiksi viiveen kasvua ja pakettien törmäämisiä. ZigBee on kehitetty vähävirtaisuuden lisäksi nopeaksi toiminnaltaan, mikä myös osaltaan pienentää virrankulutusta. ZigBeen kytkeytyminen verkkoon kestää alle 30 ms. Sleep tilasta herääminen ja lähetyksen aloittaminen tapahtuu alle 15 ms:ssa. [22.]

ZigBee käyttää kolmea eri modulaatiotekniikkaa: Direct Sequence Spread Spectrumissa (DSSS) lähetettävä sanoma jaetaan pieniin osiin ja lähetetään koko taajuusalueella yhtenä signaalina. Quadrature phase-shift keying (QPSK)- ja Binary phase-shift keying (BPSK) -tekniikoissa muutetaan kanta-aallon vaihetta niin, että se ilmaisee eri binäärisymboleita. BPSK:ssa on kaksi kanta-aaltoa ja QPSK:ssa on neljä kanta-aaltoa. [24.]

ZigBee-verkko koostuu yleensä useista laitteista. Jos kaikki laitteet yrittävät lähettää tietoa toisistaan tietämättöminä, voi tapahtua datan törmäämistä. Jotta näin ei pääsisi tapahtumaan, käytetään CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) [19] -menetelmää (kuva 10).



Kuva 10. RTS/CTS-paketin törmäyksenestön toiminta yksinkertaistettuna [35].

Kun laite haluaa lähettää sanoman, se kuuntelee ensin, onko siirtotie vapaa ja pysyykö se vapaana DIFS (distributed interframe space) -viiveen ajan. Mikäli laite havaitsee liikennettä, se siirtyy eksponentiaaliseen toipumistilaan eli tilaan, jossa se odottaa satumanvaraisen ajan ja palaa kuuntelemaan, onko siirtotie vapaa. Jos siirtotie kuulostaa vapaalta, laite pyytää tukiasemalta lupaa lähettää data lähettämällä RTS (Request To Send) -pakettin. Jos tukiasemalta ei tule CTS (Clear To Send) -kuittaus SIFS (short interframe space) -viiveen kuluessa, olettaa laite RTS- tai CTS-paketin törmänneen, ja se siirtyy takaisin eksponentiaaliseen toipumistilaan. Jos laite saa CTS-kuittauksen, se

lähettää alkuperäisen datan, minkä jälkeen laite jää odottamaan kuittausta ACK-sanoman perillemenosta tukiasemalta SIFS-viiveen ajaksi. Jos laite ei saa ACK:ta, se olettaa, että sanoma törmäsi ja laite siirtyy jälleen eksponentiaaliseen toipumistilaan ja aloittaa kaiken uudelleen alusta. [24.]

4.2 Toimintamuodot

802.15.4-standardi määrittelee kaksi erilaista laitetyyppiä, ne ovat FFD (Full Function Device) ja RFD (Reduced Function Device) [24].

FFD-laite toimii tyypillisesti verkon hallitsijana ja koordinaattorina, jonka tehtäviin kuuluu verkon muodostus ja ylläpito. Se tukee standardin kaikkia ominaisuuksia. Se voi myös toimia koordinaattorin ja reitittimen lisäksi päätelaitteena. FFD-laite voi olla yhteydessä toiseen FFD-laitteeseen tai RFD-laitteeseen.

RFD-laite on nimensä mukaisesti karsittu versio FFD-laitteista ja käyttää vain standardin tärkeimpiä ominaisuuksia. Se on suoraan vuorovaikutuksessa sovelluksiin, antureihin tai kytkimiin, eli se on verkon päätelaite. RFD on nimensä mukaisesti riisuttu laite kaikesta ylimääräisestä, jolloin virrankulutus saadaan alhaiseksi. RFD on huomattavasti pienitehoisempi kuin FFD, ja se voi olla suoraan yhteydessä vain FFD-laitteeseen.

ZigBee-verkossa toimii kolmenlaisia laitteita, koordinaattori (FFD), reitittäjiä (FFD) ja päätelaitteita (RFD).

Koordinaattori

Koordinaattori on verkon hallitsija. Niitä on yksi jokaisessa ZigBee-verkossa. Koordinaattori on aina FFD-laite. Koordinaattori valitsee verkon kanavan ja PAN (Personal Area Network) ID:n luodakseen verkon. Se on myös vastuussa osoitteiden valinnasta. Uudet laitteet voivat liittyä verkkoon milloin vain, kun koordinaattori on aktiivinen. Koordinaattorin ollessa suljettuna uudet laitteet eivät voi liittyä verkkoon, mutta siellä jo olevat ja osoitteen omaavat laitteet pystyvät toimimaan tavalliseen tapaan. Koordinaattori voi vastaanottaa ja reitittää dataa eteenpäin, mutta ei voi mennä sleep-tilaan. Suuren virrankulutuksen takia sen optimaalinen virtalähde on verkkovirta. [25.]

Reititin

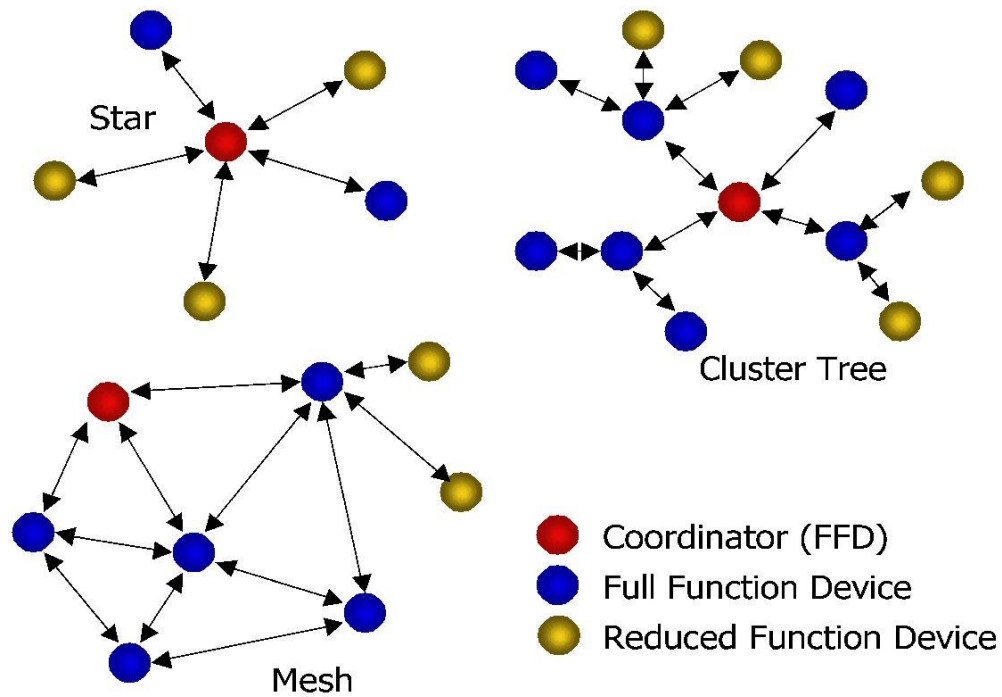
Reitittimen täytyy ensimmäiseksi liittyä olemassa olevaan ZigBee-verkkoon, ennen kuin se voi alkaa vastaanottaa ja reitittää dataa. Se ei voi mennä lepotilaan, vaan tarvitsee verkkovirran toimiakseen optimaalisesti. Reititin on aina FFD-laite. Reitittimien määrää verkossa ei ole rajoitettu. [25.]

Päätelaite

Päätelaite eli end device voi olla esimerkiksi sensori, kytkin, rele tai jokin muu vastaava laite, jolla on yleensä tarkasti määritelty tehtävä. Sen on liityttävä olemassa olevaan verkkoon, ennen kuin se voi alkaa lähettää dataa. Päätelaite voi olla yhteydessä vain koordinaattoriin tai reitittimeen. Päätelaite ei voi olla yhteydessä toiseen päätelaitteeseen eikä liittää muita laitteita verkkoon, vain reititin ja koordinaattori voivat tehdä niin. Päätelaite ei reititä dataa, vaan se voi ainoastaan lähettää tai vastaanottaa sitä. Päätelaitteen tärkein ominaisuus on sen mahdollisuus vaipua sleep-tilaan, eli silloin virrankulutus laskee merkittävästi. Tällöin päätelaite säästää virtaa ja voi toimia pitkiäkin aikoja ilman akun vaihtoa. Päätelaite on tarkoitettu akulla toimivaksi, jolloin se voidaan sijoittaa paikkoihin, joissa ei ole mahdollista saada käyttöön verkkovirtaa. Päätelaite voi olla FFD- tai RDF-laite. [25.]

4.3 Verkkotopologiat

ZigBee-tekniikassa käytetään kolmea erilaista topologiaa: ne ovat tähti-, cluster- ja mesh-topologia [26] (kuva 11).



Kuva 11. Zigbeeen verkkotopologiat [27].

Tähtitopologia

Tähtitopologian verkko koostuu yhdestä koordinaattorista ja yhdestä tai useammasta päätelaitteesta tai reitittimestä. Kaikki laitteet kommunikoivat ainoastaan koordinaattorin kanssa, joten tiedonsiirrossa päätelaitteelta lähetetty tieto kulkee määränpään koordinaattorin kautta. Tähtitopologia on singlehop-tyyppinen, eli kaikki tiedonsiirrot kulkevat yhden koordinaattorin kautta, johon kaikki päätelaitteet ovat suoraan yhteydessä. Vaihtoehtoisia reittejä ei ole. [26.]

Verkon heikkoutena on, että luotettavuus kärsii helposti laitteiden määrän kasvaessa, koska silloin datan törmäämistä tapahtuu todennäköisemmin. Verkon kantama rajoittuu koordinaattorin lähetyalueelle. Suurin heikkous on koordinaattorin vikatilanne. Silloin koko verkko lakkaa toimimasta. Tähtirakenteen etuna on, ettei yhden kaapelin rikkoutuminen vaikuta muun verkon käyttöön. Kun verkkokartta on yksinkertainen, ovat laitteiden etäisyydet lyhyitä niin fyysisesti kuin hyppyjen määrässäkin katsottuna. Tällöin data liikkuu nopeasti. [26.]

Cluster-topologia

Cluster tree -topologiassa koordinaattori on yhdistetty yhteen tai useampaan reitittimeen ja/tai päätelaitteeseen. Reitittimet voivat olla yhteydessä yhteen tai useampaan reitittimeen tai päätelaitteeseen. Näin ollen verkon kantamaa ja laitteiden määrää voidaan kasvattaa merkittävästi suuremmaksi kuin tähtiverkossa. Lisäksi reitittimillä verkon laitteiden fyysistä etäisyyttä toisistaan voidaan kasvattaa niin, että päätelaitteen ei tarvitse olla koordinaattorin kanssa samalla kuuluvuusalueella toimiakseen verkossa. Reititin toimii tällöin eräänlaisena toistimena, jolloin päätelaitteen ja koordinaattorin välinen yhteys saadaan pidettyä yllä. [26.]

Cluster tree -topologia on multihop-tyyppinen, jossa tiedot välitetään joko reitittimen tai koordinaattorin kautta. Tiedon välittämiseen voi löytyä useita mahdollisia reittejä, joista reititin valitsee sopivimman vaihtoehdon. Cluster-verkkoa voidaan kuvailla moneksi tähtiverkoksi, jotka ovat yhteydessä toisiinsa koordinaattorin kautta. Koordinaattorin vikatilanteessa verkko ei suoraan lakkaa olemasta vaan muuttuu moneksi toisistaan irrallisiksi erilliseksi tähtiverkoksi. [26.]

Mesh-topologia

Mesh-topologia on muunnos edellä kuvatusta Cluster tree -topologiasta. Se on yleisimmin käytetty verkon muoto. Verkon suurimpana etuna voidaan pitää sitä, että koordinaattori ja kaikki reitittimet kykenevät yhdistymään suoraan toisiinsa radiokantaman sisällä. Päätelaitteet eivät edelleenkään pysty kommunikoimaan suoraan keskenään, mutta voivat olla yhteydessä moneen reitittimeen. Mesh-topologian etuna voidaan pitää pieniä viiveitä, koska reitittimet voivat valita sen hetken lyhyimmän ja nopeimman reitin. Etuna Cluster tree -topologian tavoin voidaan myös pitää luotettavuutta, joka taataan useilla siirrettävän tiedon reititysvaihtoehdoilla. Koordinaattorin vikatilanteessa verkko ei lakkaa toimimasta, vaikkakaan uudet laitteet eivät pysty liittymään olemassa olevaan verkkoon. [26.]

4.4 Tietoturva

ZigBee-verkot on kehitetty turvallisiksi. Niiden keskeisenä menetelmänä on pääsyylista (Access Control List), jonka toimesta vain ennalta tunnetut laitteet voivat liittyä verk-

koon. Yksinkertaisuudessaan tämä toimii niin, että verkon koordinaattori luo ja hallitsee listaa, joka sisältää sallittujen laitteiden MAC-osoitteet. Pääsyylistan lisäksi toimivana turvatoimena voidaan pitää myös Message Freshness Timer -menetelmää. Sen toiminta perustuu viestien mukana oleviin aikaleimoihin. Aikarajan ylittäneet, vanhentuneet viestit hylätään. Menetelmällä ehkäistään nauhoitetut hyökkäykset. Näitä hyökkäyksiä ovat esimerkiksi, kun hyökkääjä nauhoittaa lähetyksen ja uusii sen myöhemmin. Tällainen tilanne voi tulla, jos hyökkääjä nauhoittaa oven lukituskoodin etukäteen päästäkseen sisälle sopivana ajankohtana.

Tiedon salaukseen käytetään 128-bittistä AES (Advanced Encryption Standard) -salausmenetelmää. AES-algoritmit ovat sisäänrakennettuina ZigBee-kortteihin, joiden kautta ne myös toimivat. Kun salaus on aktivoitu, koordinaattori käynnistyy käyttäen 128-bittistä salausavainta. Tällöin ainoastaan laitteet, joilla on sama avain, pystyvät kommunikoimaan verkossa. Verkkoon liittyvillä reitittimillä ja päätelaitteilla täytyy olla tämä salausavain. Jos avainta ei ole, täytyy verkkoon pyrkivän laitteen hankkia se salaamattomalla siirrolla, josta seuraa hetkellinen tietoturva-aukko. Kaikki lähetettävä tieto salataan 16-tavuisella salausavaimella. Vastaanottopäässä kaikki salaamaton tieto hylätään. AES-salaus on tehokas osa tietoturvaa, mutta huonojakin puolia siinä on. Multihop-tyyppisessä tiedonsiirrossa reitin varrella jokaisen reitittimen kohdalla joudutaan purkamaan salaus ja sitten taas salaamaan tieto uudelleen. Seurauksena on viiveen kasvun lisäksi se, että lähetettävien pakettien koko kasvaa.

4.5 XBee-lähetin-vastaanotinmoduuli

Tässä työssä käytettiin XBeen lähetin- ja vastaanotinmoduulia (kuva 12 ja taulukko 1), ja se on ZigBee-standardiin perustuva. Se toimii 2,4 GHz:n taajuudella ja on Maxstreamin kehittämä. XBee-lähetin- ja vastaanottomoduulissa on pieni virrankulutus ja kohtuullinen hinta. Moduuliin on rakennettu myös A/D-muunnos ilman mikrokontrolleria.



Kuva 12. Xbee-moduulin nastakaavio [28].

XBeen teoreettinen kantama sisällä on noin 30 m ja ulkona noin 100 m, kun laitteiston välillä ei ole esteitä. Tähän se käyttää 1 mW:n tehon. Radiolinkin tiedonsiirtotasoa on 250 000 bittiä sekunnissa ja se toimii 2,8–3,4 V:n jännitteellä. Lähetysvirtana on 45 mA:n jännite. [28.]

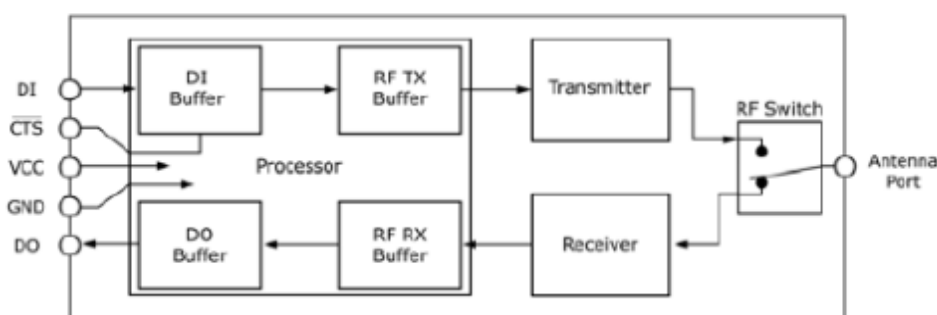
Taulukko 1. XBee-moduulin nastakaavio [28].

Pin #	Name	Direction	Description
1	VCC	-	Power supply
2	DOUT	Output	UART Data Out
3	DIN / CONFIG	Input	UART Data In
4	DO8*	Output	Digital Output 8
5	RESET	Input	Module Reset (reset pulse must be at least 200 ns)
6	PWM0 / RSSI	Output	PWM Output 0 / RX Signal Strength Indicator
7	PWM1	Output	PWM Output 1
8	[reserved]	-	Do not connect
9	DTR / SLEEP_RQ / DI8	Input	Pin Sleep Control Line or Digital Input 8
10	GND	-	Ground
11	AD4 / DIO4	Either	Analog Input 4 or Digital I/O 4
12	CTS / DIO7	Either	Clear-to-Send Flow Control or Digital I/O 7
13	ON / SLEEP	Output	Module Status Indicator
14	VREF	Input	Voltage Reference for A/D Inputs
15	Associate / AD5 / DIO5	Either	Associated Indicator, Analog Input 5 or Digital I/O 5
16	RTS / AD6 / DIO6	Either	Request-to-Send Flow Control, Analog Input 6 or Digital I/O 6
17	AD3 / DIO3	Either	Analog Input 3 or Digital I/O 3
18	AD2 / DIO2	Either	Analog Input 2 or Digital I/O 2
19	AD1 / DIO1	Either	Analog Input 1 or Digital I/O 1
20	AD0 / DIO0	Either	Analog Input 0 or Digital I/O 0

4.6 XBee-moduulin käyttö ja komennot

XBee-moduuleihin on sisäänrakennettu kontrollilogiikka, joten XBeetä ohjataan valmistajan tarjoamilla yksinkertaisilla komennoilla. Komennot lähetetään moduulille samalla lailla kuin data. XBeen oma ohjelmisto osaa erottaa datan ja käyttäjän antamat komennot toisistaan siitä, että se laitetaan "odota komentoa" -tilaan lähettämällä kolme plusmerkkiä. Komennot lähetetään ASCII-merkkeinä. XBeehin lähetettävän informaation pitää olla sarjamuotoista ja sisältää aloitusbitti, kahdeksan databittiä ja lopetusbitti. Se ottaa tämän vastaan DIN-nastan kautta ja DOUT-nasta kautta lähettää isännälleen dataa asynkronisena datavirtana.

Langaton radiolinkki on half-duplex-tyyppinen (kuva 13). Tämä tarkoittaa sitä, että yhdellä antennilla sekä lähetetään että vastaanotetaan dataa, mutta ei samaan aikaan. XBeehin on kuitenkin rakennettu ratkaisu, jonka ansiosta sillä voi lähettää ja vastaanottaa melkein samanaikaisesti: Samalla jos lähetetään ja vastaanotetaan dataa, lähetettävä data varastoidaan lähetyspuskuriin ja lähetetään heti, kun vastaanotto on loppunut. Dataa voidaan vastaanottaa kuitenkin RF-linkin ja sarjaliitännän kautta samanaikaisesti. Tämän mahdollistaa ohjelmistopuskuri (100 tavua) DI-nastan jälkeen, johon se varastoi tulevan datan ja lähettää sen sitten antennilla eteenpäin. Vastaavasti DO-nasta varastoi antennilla vastaanotetun datan, ennen kuin se lähetetään isäntälaitteelle. CTS-nasta ilmoittaa isäntälaitteelle, jos lähetyspuskuri on täyttymässä. Tällöin CTS-nasta menee loogiseen ykköstitilaan, kun puskuuri sisältää 83 tavua, jolloin se ilmaisee isäntälaitteelle, että se lopettaa tiedon tuomisen puskuuriin. Loogiseen nolleen nosta palaa, kun datamäärä on laskenut 66 tavuun. TRS-nastan ollessa ykköstitilassa myös vastaanottopuskuri lopettaa datan lähettämisen isäntälaitteelle. Näin ollen vastaanottopuskuri saattaa täytyä ja tieto tuhoutua.



Kuva 13. Xbeeen sisäinen lohkoakaavio [28].

XBeelle ei voi antaa mitään komentoja, ennen kuin se on laitettu "odota komentoa" -tilaan eli lähettämällä sille kolme plus-merkkiä (hex 2B). Tämän jälkeen moduulille voi lähettää komennon. Se alkaa aina kirjaimin AT (attention). Tämän jälkeen annetaan itse komento ja komennon parametrit. Komentorivin päättää rivin alkuun palautus eli kirjainyhdistelmä CR (carriage return). XBeeltä tulee OK, jos kaikki onnistui, tai ERROR, jos se ei jostain syystä kyennyt suorittamaan käskyä. Muissa tapauksissa moduuli ei reagoi mitenkään.

Maxstream on kehittänyt XBeelle ilmaisen graafisen käyttöliittymän X-CTU:n. Tässä työssä käytin sitä. X-CTU on helppokäyttöinen ohjelma Xbeeen hallintaan. Se on selkeä, ja sillä voi antaa helposti käskyjä ja tehdä testejä XBee-moduulille.

5 ZigBee ja LabVIEW -kotiautomaatiototeutus

Insinööriyön osana tein esimerkkinä käytännön kotiautomaatiototeutuksen, jossa koekelin ZigBee-moduulien ja LabVIEW'in yhteensopivuutta ja toimintaa käytännössä. Käytin kahta XBee nodea, LM35-lämpötila-anturia, LabVIEW-ohjelmistoa käyttöliittymänä ja X-ctu:ta ZigBeen hallintaan. ZigBee-verkon testaamista varten muodostin point-to-point-verkon kahdella XBee-modulilla, jossa toinen moduuli toimi päätelaitteenä lähettäen lämpötilatietoa LM35-anturilta. Toinen oli koordinaattori, ja se vastaanotti ensimmäisen noden lähettämän datan ja välitti sen USB:n kautta Windowsilla käynnissä olevalle LabVIEW-ohjelmalle. Ensimmäinen node käytännössä olisi toiminut akulla, jolloin se olisi ollut liikuteltavissa vapaasti radion kantaman puitteissa. Verkon toiminnan tutkimista varten käytettävällä virtalähteellä ei ollut merkitystä, joten otin siihen virran USB-kaapelia pitkin. Koordinaattorimoduuli oli kytketty tietokoneeseen USB-kaapelilla. Akku ei olisi ollut vaihtoehto koordinaattorille, koska sen virrankulutus on sen verran suuri ja sitä ei yleensä tarvitse sijoittaa sellaiseen paikkaan, mihin verkkovirta ei ylettäisi. [29.]

5.1 ZigBee-verkon koordinaattorin ja päätelaitteen asetukset

Koordinaattorille ei tässä tapauksessa tarvinnut määrittää muuta kuin verkon ID ja vastaanottavan laitteen osoitteen (kuva 14), koska laitteita oli vain kaksi. Muussa tapauksessa koordinaattorilla voi lähettää broadcast-viestin asettamalla osoitteen DH 0x00 ja DL 0xFFFF. ID määrittää sen, että kaikki laitteet ovat samassa verkossa, jolloin ne voivat kommunikoida toistensa kanssa. Koordinaattori oli yhteydessä päätelaitteeseen radioteitse ja tietokoneeseen USB-portin kautta.

ID PAN ID	B1
DH Destination Address High	13A200
DL Destination Address Low	40AC4CE5

Kuva 14. Koordinaattorille asetettavat arvot.

Päätelaitteelle pitää antaa saman PAN ID kuin koordinaattorille ja koordinaattorin osoite, jolloin koordinaattori voi liittää sen verkkoon (kuva 15). Datan lähetyksen aloittamiseksi tarvitsi asettaa portti, josta vastaanotettava data tulee, ja määrittää, minkälai-

nessa muodossa. Tässä tapauksessa se oli analogista lämpötiladataa, joten asetin portin nro 0 ”muunnos analogisesta digitaaliseen muotoon (ADC)”. Tämän jälkeen vielä asetetaan näytteenoton tiheys, jolloin vältetään turhaa virrankulutusta. Päätin käyttää 1 s:a, koska halusin nähdä nopeat vaihtelut, kun sensoria lämmitti. Tämä oli sisätilan mittaavalle anturille aivan liian nopea loppukäyttäjän tilanteessa. Käytännön sovelluksessa arvo asetettaisiin johonkin yhden ja kymmenen minuutin välillä. Päätelaitteeseen oli kytketty Lm35-anturi niin, että se oli asetettu porttiin nro 0. Se välitti tietoa ZigBee-verkon välityksellä koordinaattorille.

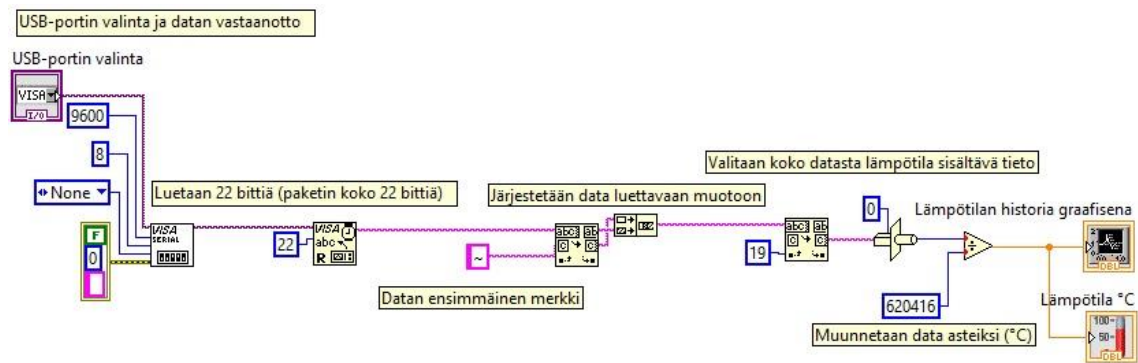
ID PAN ID	B1
DH Destination Address High	13A200
DL Destination Address Low	40AC4C4C
D0 AD0/DIO0 Configuration	ADC [2]
IR IO Sampling Rate	3E8 x 1 ms

Kuva 15. Päätelaitteelle asetettavat arvot.

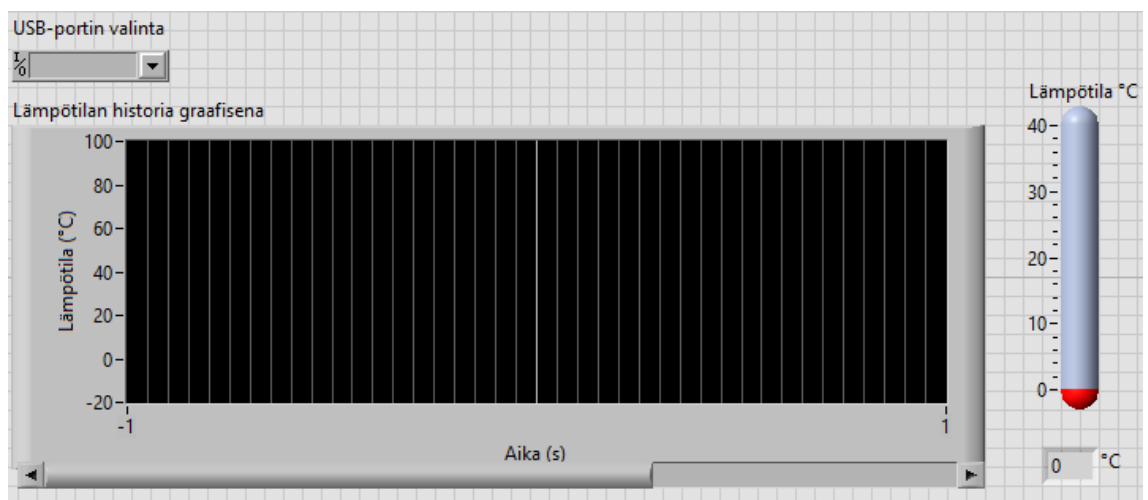
5.2 LabVIEW-ohjelma

Käyttöliittymä suunniteltiin selkeäksi ja yksinkertaiseksi verkon testaamista varten. Käytännön sovelluksissa käyttöliittymän suunnittelu pitäisi toteuttaa loppukäyttäjän tarpeiden mukaan, jolloin vaatimukset olisivat huomattavasti tarkemmat käytettävyyden suhteen.

Ohjelma on yksinkertaisuudessaan datan vastaanotto valitusta USB-portista, minkä jälkeen luetaan koko paketti eli 22 bittiä (kuva 16). Sen jälkeen nämä bitit järjestetään oikeaan järjestykseen, jotta voidaan seuraavassa kohdassa valita lämpötilan sisältävä data ja muuntaa se celsiusasteiksi ja tuoda käyttäjälle näkyviin. (Kuva 17.)



Kuva 16. LabVIEW-ohjelma koodi.



Kuva 17. LabVIEW-ohjelman käyttöliittymä.

Huonelämpötilaa mitattiin määritellyllä 1 sekunnin lähetysvälillä vuorokauden ajan lämmittäen anturia hetkittäin korkeampaan lämpötilaan. Testeissä todettiin, että tiedon siirto oli luotettavaa ja verkon muodostaminen ja LabVIEW-ohjelman kehittäminen suoraviivaista. Kehitettyä testiympäristöä laajentamalla olisi mahdollista rakentaa esimerkiksi kotiautomaation soveltuva järjestelmä.

6 BLE:n ja ZigBeen vertailu

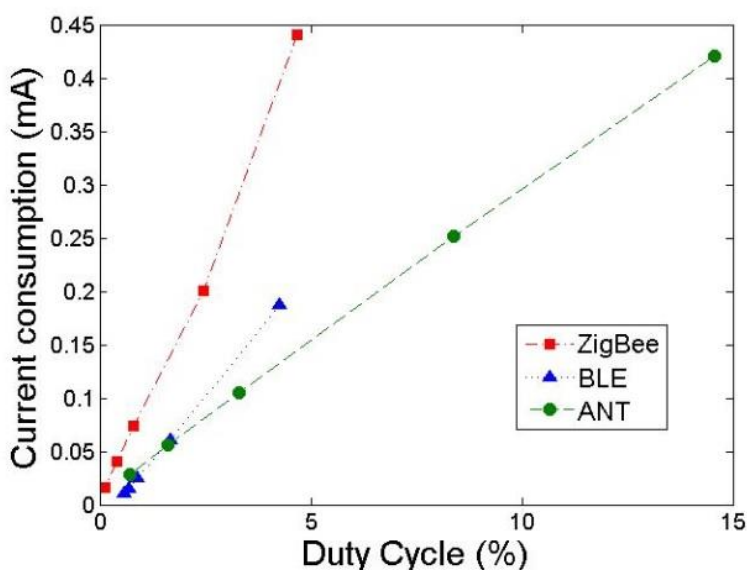
Vertailen ZigBeetä ja BLE:tä keskenään muun muassa virrankulutuksessa, etäisyydessä ja tietoturvasa. Kotiautomaatiossa nämä ovat tärkeimpiä ominaisuuksia, mitä tarvitaan. Ei välttämättä tässä järjestyksessä, mutta riippuen tarpeista. Esimerkiksi BLE-

hiiren tietoturvan ei tarvitse olla yhtä jyrkää kuin ZigBee-verkossa toimivan ulko-oven lukon.

Laitteen tärkeimmät ominaisuudet kotiautomaatiossa ovat lähes poikkeuksetta yksilöllisiä, koska kaikilla on oma tehtävä tai tehtäviä. Tavallisesti jokaisella päätepisteen laitteella on vain yksi tarkka tehtävä, esimerkiksi lämpötilan mittaaminen. Lisäksi on voitu lisätä kosteuden mittaus ja muita vastaavia toimintoja.

Virrankulutus

Kuvan 18 suuntaa antavista arvoista voidaan todeta, että keskimäärin BLE:n virrankulutus on noin puolet alhaisempi kuin ZigBeellä. Lopulliseen virrankulutukseen kuitenkin vaikuttaa lähetysteho, häiriöiden määrä, etäisyys ja lähetettävän datan koko, joten tästä taulukosta ei voi vetää lopullisia johtopäätöksiä.



Kuva 18. ZigBeen ja BLE:n virrankulutuksen vertailu suhteessa keskenään ja ANT-järjestelmään, joka on pelkästään sensoriverkkoon optimoitu järjestelmä. Keskimääräinen virrankulutus vasemmassa reunassa (mA). Duty cycle on keskimääräinen hereilläoloaika jaettuna kokonaisen paketin lähettämiseen tarvittaviin toimenpiteisiin kuluneella ajalla. [30.]

Tietoturva

Molemmassa järjestelmissä tietoturvan taso on erittäin korkea. Niissä on monta sisäänrakennettua turvatasoa ja mekanisme, jotka huolehtivat tarvittavasta tietoturvasta. ZigBee käyttää muun muassa access control list- ja freshness timer -mekanismeja.

BLE:ssä taas on käytössä pairing-, bonding- ja Encryption Re-establishment -metodi. Molempien dataliikenne salataan käyttämällä 128 AES-bittistä salausta.

Käytännön eroja

ZigBee- ja BLE-järjestelmät ovat toiminnaltaan ja ominaisuuksiltaan monilta osin samankaltaisia. Isoimpana erona on virrankulutus, joka on ZigBeessä selvästi suurempi ja suurin heikkous BLE:hen verrattuna (taulukko 2). Myös datanopeus on korkeampi BLE:ssä kuin ZigBeessä, ja verkon latenssi on pienempi BLE:ssä. Nopealla johtopäätöksellä voisi jo todeta, että BLE olisi ylivoimainen ZigBeehen verrattuna.

Taulukko 2. BLE:n ja ZigBeen välinen vertailu [2; 3; 28].

	BLE	ZigBee
Datanopeus	1 Mbit/s	20, 40 ja 250 kbits/s
Etäisyys	noin 10 m	noin 10–100 m
Taajuus	2,4–2,483 GHz	868 Mhz, 900–928 MHz, 2,4 GHz
Virrankulutus	Erittäin pieni (ks. kuva 18)	Pieni (ks. kuva 18)
Verkkotopologia	tähti, P2P	tähti, cluster tree, mesh
Kanavien lkm	40	16
Kanavan leveys	2 MHz	2 MHz
Max nodejen lkm	7	65 000
Standardi	Bluetooth core 4.0	IEEE 802.15.4
Latenssi	6 ms	30 ms–1 s

ZigBee on kuitenkin selvästi kehittyneempi verkkotopologioissa, koska se tukee mesh-topologiaa. Mesh-topologia on ylivertainen, kun verkossa on useampia reitittimiä tai koordinaattoreita. Bluetooth SIG on kuitenkin tuomassa vuonna 2016 suuren päivityksen, jossa on tuki mesh-verkoille. Samassa päivityksessä kantaman pitäisi nelinkertaistua ja tiedonsiirtonopeuteen luvataan 100 prosentin parannus. ZigBeessä on ainakin tällä hetkellä suurempi kantama, ja kun sen yhdistää mesh-verkkotopologiaan, BLE ei olekaan enää edellä, vaan jopa askeleen takana. [14.]

Loppuanalyysi

Tutkittuani Bluetooth low energy- ja ZigBee-järjestelmää ja vertailllessani niiden ominaisuuksia huomasin, kuinka erilaiset ne loppujen lopuksi ovat, koska ZigBee on alusta lähtien kehitetty mesh-topologiaa varten ja BLE on alun perin kehitetty point-to-point-topologia varten. Niiden käyttötarkoituksia voi erota paljon. Molemmat voivat optimaalisissa olosuhteissa toimia jopa vuosia ilman akun vaihtoa, ja niiden datanopeus on pieni.

Molemmat protokollat on optimoitu minimoimaan virrankulutus, mikä on yksi tärkeimmistä ominaisuuksista kotiautomaatiossa. Monesti kotona verkon kautta ohjattavat laitteet ovat pieniä ja tiettyä toimintoa varten kehitettyjä, esimerkiksi lämpömittari, joka usein sijoitetaan sellaiseen paikkaan, että verkkovirta on kustannustehokkuuden näkökulmasta huono idea yhdistää siihen. ZigBee on kuitenkin heikompi virrankulutuksessa verrattuna BLE:hen. ZigBee tukee mesh-verkkotopologiaa, joten sillä saa huomattavasti laajemman solmupisteiden määrässä laskettuna ja näin ollen varmemman verkon. ZigBeen etuna on myös selvästi suurempi kantama BLE:hen verrattuna, jolloin tarvitaan vähemmän laitteita samankokoisen alueen peittämiseen. Tässä etuna on selvästi suurempi datan lähetyskapasiteetti, eli heti, kun tarvitaan pitempää kantamaa, BLE jää auttamatta jälkeen.

Lähitulevaisuudessa BLE:n markkinaosuus saattaa merkittävästi kasvaa jopa markkinoita hallitsevaksi järjestelmäksi. Merkittävänä tekijänä tähän pidän sitä, että BLE on selvästi edellä virrankulutuksessa ja yksinkertaisuudessa verrattuna ZigBeehen. Toinen merkittävä tekijä on BLE:n tuki erilaisissa ja eri valmistajien mobiililaitteissa, siinä missä ZigBee on edelleen lähinnä teollisuussovelluksissa käytetty järjestelmä.

Vastaavasti myös Zigbeeen osuus kasvaa kotiautomaatiomarkkinoiden kehityksen vuoksi nyt ja tulevaisuudessa. Suuremman potentiaalin omaavana BLE:llä on kuitenkin mielestäni tulevaisuudessa suuremmat mahdollisuudet kasvaa. Vaikka BLE ei vielä tue mesh-verkkotopologiaa, heti sen jälkeen kun Bluetooth SIG saa tuen valmiiksi, on ZigBee askeleen heikomi. Tällä hetkellä on selvästi kasvua WPAN-laitteilla ja niitä suunnitellaan yhä enemmän. Tekniikan pienentyessä saadaan enemmän laitteita ihmisen henkilökohtaiseen verkkoon mukaan, jolloin virrankulutus ja akkujen koko on yksi merkittävimmistä tekijöistä. [4.]

Näkisin, että tulevaisuudessa ZigBee jää BLE:n jalkoihin, koska jo pelkästään BLE:llä on valtavasti suurempi koneisto kehittämässä protokollaa. BLE on myös jo tällä hetkellä ZigBeetä edellä monessa tärkeässä osa alueessa pois lukien mesh-topologia. ZigBeelle varmasti jatkossakin on oma ostajakunta, koska se on avoimeen järjestelmään perustuva, kun taas BLE on täysin suljettu ekosysteemi.

7 Yhteenveto

Insinööriyössä tutkin ZigBeetä ja BLE:tä, ja vertailin niitä keskenään. Tutkimuksen kohteet eivät olleet minulle ennestään tuttua, ja opin paljon molemmista järjestelmistä. Työ oli paljolti yksin työskentelyä ja tutkimista. Se myös haastoi minua miettimään aikataulua ja tiedon etsimiseen käytettäviä keinoja. Vastoinkäymiset eivät estäneet minua ja sain tehtyä esimerkkisovelluksen ja kirjoitettua tutkimuksen molemmista järjestelmistä.

Lisäksi tein työssä esimerkki kotiautomaatitoteutuksen käyttämällä ZigBeetä ja LabVIEW'ia. Siinä opin paljon lisää ZigBeestä käytännössä. LabVIEW on ennestään tuttu ja siinä ongelmaksi tuli ZigBeen kanssa kommunikointi, jonka sain lopulta ratkaistua. ZigBeetä on helppo konfiguroida käyttämällä X-CTU:n luomaa käyttöliittymää, mistä ei suuremmin ongelmia syntynyt, kun seurasi ZigBeen konfiguraatio ohjeita. Lopputuloksena sain luotua yksinkertaisen verkon ja siihen käyttöliittymän LabVIEW'illä.

Lähteet

1. Bluetooth low energy. 2016. Verkkodokumentti. Bluetooth SIG.
<<https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy>> Luettu 2.2.2016.
2. Kooker, John. 2008. Bluetooth, ZigBee, and Wibree: A Comparison of WPAN Technologies. Verkkodokumentti.
<https://cseweb.ucsd.edu/classes/fa08/cse237a/topicresearch/jkooker_tr_report.pdf> Luettu 3.2.2016.
3. Davidson Robert, Akiba, Cufi Carles, Townsend Kevin. 2014. Getting Started with Bluetooth Low Energy. E-kirja. Safari.
<<https://www.safaribooksonline.com/library/view/getting-started-with/9781491900550/ch01.html>> Luettu 10.2.2016.
4. Nilsson, Rolf. 2011. Bluetooth Low Energy Technology Makes New Applications Possible. Verkkodokumentti. Digi-Key Corporation.
<<http://www.digikey.com/en/articles/techzone/2011/dec/bluetooth-low-energy-technology-makes-new-applications-possible>> Luettu 12.2.2016.
5. TI's Bluetooth™ & Bluetooth Smart / Bluetooth low energy (BLE) solutions. Verkkodokumentti. Texas Instruments.
<http://www.ti.com/lscds/ti/wireless_connectivity/bluetooth_ble/overview.page?DCMP=BluetoothLowEnergy&HQS=Bluetoothlowenergy> Luettu 13.2.2016.
6. Bluetooth low energy. 2011. Verkkodokumentti. Glyn Store.
<http://www.glynstore.com/content/docs/bluegiga/BLE_getting_started.pdf> Luettu 20.2.2016.
7. Bennett, Brian. 2012. The power of Bluetooth 4.0: It'll change your life. Verkkodokumentti. CBS Interactive Inc. <<http://www.cnet.com/news/the-power-of-bluetooth-4-0-itll-change-your-life/>> Luettu 15.1.2016.
8. Bluetooth devices. 2016. Bluetooth SIG.
<<http://www.bluetooth.com/Pages/Bluetooth-Smart-Devices-List.aspx>> Luettu 20.1.2016.
9. Ren, Kai. 2015. Ten Important Differences between Bluetooth BR/EDR and Bluetooth Smart. Verkkodokumentti. Bluetooth SIG.
<<http://blog.bluetooth.com/ten-important-differences-between-bluetooth-bredr-and-bluetooth-smart/>> Luettu 7.2.2016.
10. Pitkänen, Manu. 2014. Tämä on uutta Bluetooth 4.2:ssa. Verkkodokumentti. AfterDawn Oy. <<http://www.hardware.fi/uutiset/artikkeli.cfm/2014/12/04/tama-on-uu-tta-bluetooth-4-2>> Luettu 7.2.2016.

11. O'Brien, Terrence. 2011. iPhone 4S claims title of first Bluetooth 4.0 smartphone, ready to stream data from your cat. Verkkodokumentti. AOL Inc. <<http://www.engadget.com/2011/10/12/iphone-4s-claims-title-of-first-bluetooth-4-0-smartphone-ready/>> Luettu 20.3.2016.
12. Gervasi, Charles. 2013. Bluetooth Low Energy. Verkkodokumentti. Premier Farnell plc. <<https://www.element14.com/community/groups/wireless/blog/2013/08/23/bluetooth-low-energy>> Luettu 10.1.2016.
13. Scatternet – Part 1. 2004. Verkkodokumentti. Bluetooth SIG. <https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0CDwQFjAHahUKEwjvnrTNhdvIAhXMEywKHR5UBko&url=https%3A%2F%2Fwww.bluetooth.org%2Fdocman%2Fhandlers%2FDownloadDoc.aspx%3Fdoc_id%3D40335&usq=AFQjCNEE1107C73WA4jGJ4B90FjyxgqQ&sig2=rETnLYs12NX6O4W8w3v_Og> Luettu 18.3.2016.
14. Pitkänen, Manu. 2015. Bluetooth saa ison päivityksen – kuuluvuus nelinkertaistuu. Verkkodokumentti. AfterDawn Oy. <<http://www.hardware.fi/uutiset/artikkeli.cfm/2015/11/16/bluetooth-saa-ison-paivityksen-kuuluvuus-nelinkertaistuu>> Luettu 6.3.2016.
15. Qusay H. 2003. Mahmoud Wireless Application Programming with J2ME and Bluetooth. Verkkodokumentti. Oracle. <<http://www.oracle.com/technetwork/java/javase/downloads/index-156651.html>> Luettu 24.1.2016.
16. Rowberg, Jeff. 2013. Bonding, encryption, and MITM protection with BLE modules. Verkkodokumentti. Bluegiga. <<https://bluegiga.zendesk.com/entries/22882472--REFERENCE-Bonding-encryption-and-MITM-protection-with-BLE-modules>> Luettu 4.2.2016.
17. Bluetooth 4.0 Single Mode Modules. Verkkodokumentti. BlueRadios, Inc. <http://www.blueradios.com/hardware_LE4.0-S2.htm> Luettu 14.2.2016.
18. Technical considerations for Bluetooth low energy application developers. 2016. Verkkodokumentti. Bluetooth SIG. <<https://www.bluetooth.com/specifications/bluetooth-core-specification/technical-considerations>> Luettu 3.3.2016.
19. IEEE 802.15 WPAN™ Task Group 4 (TG4). 2016. Verkkodokumentti. IEEE. <<http://www.ieee802.org/15/pub/TG4.html>> Luettu 2.3.2016.
20. Frenzel, Lou. 2013. What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?. Verkkodokumentti. Penton. <<http://electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless>> luettu 11.11.2015.

21. Light+Building. 2016. Verkkodokumentti. OPTOGA AB.
<<http://www.optoga.com/en/lightbuilding-2016/>> Luettu 21.11.2015.
22. Gratton, Dean Anthony. 2013. The Handbook of Personal Area Networking Technologies and Protocols. E-kirja. Cambridge University Press.
<https://books.google.fi/books?id=XpGAAAAQBAJ&printsec=frontcover&hl=fi&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=true> Luettu 1.12.2015.
23. Zigbee: A Global Wireless Standard. 2011. Verkkodokumentti. Digi-Key Corporation. <<http://www.digikey.com/en/articles/techzone/2011/aug/zigbee-a-global-wireless-standard>> Luettu 17.11.2015.
24. Part 15.4: Low-Rate Wireless Personal Area Networks. 2011. Verkkodokumentti. IEEE. <<https://standards.ieee.org/getieee802/download/802.15.4-2011.pdf>> Luettu 14.11.2015.
25. ZigBee home automation public application profile. 2013. verkkodokumentti. ZigBee Alliance. <<http://www.zigbee.org/non-menu-pages/zigbee-home-automation-download/>> Luettu 12.12.2015.
26. Introduction to Zigbee Technology. 2011. Verkkodokumentti. Premier Farnell plc.
<<https://www.element14.com/community/servlet/JiveServlet/previewBody/37177-102-1-219424/Introduction%20to%20Zigbee%20Technology.pdf>> Luettu 14.11.2015.
27. ZigBee SoCs provide cost-effective solutions. 2005. Verkkodokumentti. UBM LLC. <http://www.eetimes.com/document.asp?doc_id=1273396> Luettu 3.11.2015.
28. XBee datasheet. 2009. Verkkodokumentti. Digi International Inc.
<<https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf>> Luettu 24.11.2015.
29. LM-35 datasheet. 2016. Verkkodokumentti. Texas Instruments.
<<http://www.ti.com/lit/ds/symlink/lm35.pdf>> Luettu 14.11.2015.
30. Dementyev Artem, Hodges Steve, Taylor Stuart ja Smith Joshua. 2013. Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario. Verkkodokumentti. Microsoft Research.
<<http://research.microsoft.com/pubs/192688/IWS%202013%20wireless%20power%20consumption.pdf>> Luettu 27.3.2016.
31. Smith, Phil. 2011. Comparing Low-Power Wireless Technologies. Verkkodokumentti. Digi-Key Corporation.
<<http://www.digikey.com/en/articles/techzone/2011/aug/comparing-low-power-wireless-technologies>> Luettu 16.2.2016.

32. What's The Difference Between Bluetooth Low Energy And ANT?. 2012. Verkkodokumentti. Penton. <<http://electronicdesign.com/mobile/what-s-difference-between-bluetooth-low-energy-and-ant>> Luettu 13.1.2016.
33. Chu, David. 2013. Core Bluetooth on iOS. Verkkodokumentti. LinkedIn Corporation. <<http://www.slideshare.net/storywithoutend/core-bluetooth-on-ios>> Luettu 10.1.2016.
34. Bluetooth Smart (Low Energy) Technology. Verkkodokumentti. Bluetooth SIG. <<https://developer.bluetooth.org/TechnologyOverview/Pages/BLE.aspx>> Luettu 1.3.2016.
35. Carrier sense multiple access with collision avoidance. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance> Luettu 20.3.2016.